# Formulating a Complex Solution to Secure Data in Information Systems for Supply Chain Management

Veenababu Kannika Sherly

Research Analyst, SMRVD Security Solutions, India.

**Abstract**

To successfully integrate business processes between suppliers and customers, manufacturers must solve the complex problem of information security. IoT is defined as a group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to data they generate. It embodies the next phase toward mass digitization of supply chains to facilitate innovations. IoT encompasses devices such as sensors as well as passive, semi-passive (or semi-active), and active electronics which are connected over a network. This research aims to investigate the current status and future direction of the use of information systems for supply chain management for companies with multicomponent production. Based on data collected from different enterprises, can be concluded that in order to identify the most effective strategies of information support of supply chain the attention should focus on the identification and management of the sources of uncertainties.

**Keywords:** Supply chain management; Anomaly based algorithm.

## 1. Introduction

Information systems are designed to automate and manage of all stages of the organization's supply maintenance and control the entire product distribution in the organization. The term was introduced in 1988, when the founders of the US-based company i2, discovered another unoccupied segment in the information system market. Since then, many suppliers offer a variety of

solutions that are marketed as those intended for supply chain management. SCM modules are in all ERP systems. The SCM system allows significantly better satisfy the demand for the company's products and significantly reduce the costs of logistics and purchasing [1-9].

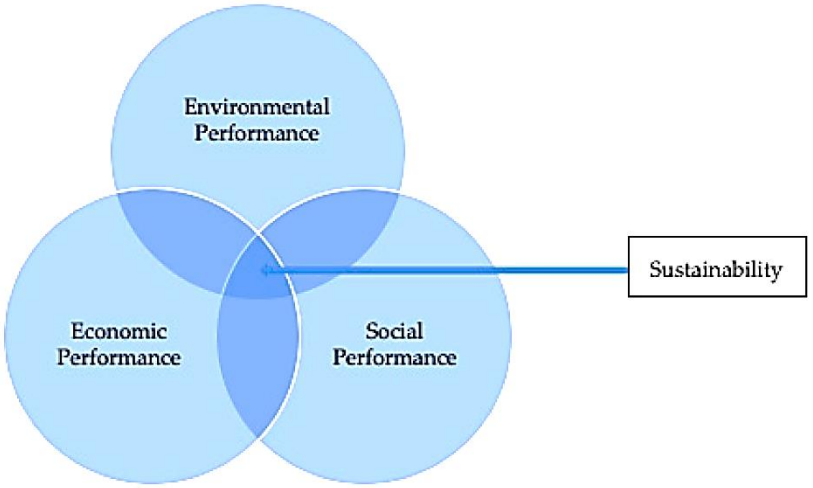


**Figure 1.** Sustainable SCM (Source: Internet)

SCM covers the entire cycle of purchasing of raw materials, production and product distribution. Generally, researchers identify six main areas that supply chain management focuses on: production, supplies, location, warehouse inventory, transportation, and information. The following tasks are implemented:

- Improvement of service level.
- Optimization of the production cycle Reducing of warehouse inventory.
- Improvement of enterprise productivity Rise of profitability.
- Control of the production process.

**2. SCM Solutions**

SCM solutions create optimal plans for the use of existing technological lines detailing what, when and in what sequence should be made taking into

account the limitations of capacity, raw materials and materials, batch sizes and the need to change equipment to produce a new product. This helps to achieve a high satisfaction of demand at minimum cost. According to AMR Research and Forrester Research, the implementation of SCM allows the companies gain such competitive advantages as reducing the cost and order processing time (by 20-40%), reducing purchasing costs (by 5-15%), reducing time to market (by 15% -30%), reducing the warehouse inventory (by 20-40%), reducing the production costs (by 5-15%), increase in profits by 5-15%.

A well-functioning supply chain helps to improve the planning system, optimize warehouse inventory, make timely deliveries, ensure offer to demand conformity, reduce costs and, as a result, increase the company's market value.

The current trends in the development of SCM technologies are defined by the enormous possibilities of the Internet [10-27]. The chains of manufacturers, suppliers, contractors, transport and trading companies are intertwined in the most intimate way and are already real online networks. Companies merge into the business community, and the boundaries between them are disappeared. However, there is a transparency of joint activities, performers can quickly adapt to customer requirements, as well as quickly bring new products to the market using advanced methods of prediction and planning.

The Internet is the simplest, cheapest, and most efficient technological means to manage and control the partner networks. Companies usually start with combination of the simplest activities using emails and workflow automation systems, then moving on to virtual docking of the most important business processes, and then merging into one virtual corporation within which the entire network is synchronized [28-33]. This is already a transition to global e-commerce, when all business transactions and payments are arranged through the Web without exception. As a result, not only productivity significantly

increases, but also all processes significantly accelerate which lead to qualitatively new effects. For example, such a network system can minimize the impact of almost any negative external influences and create new products much faster than competitors. One of the first corporations that successfully switched to the parallel design of their products (laser printers) by uniting development teams from different countries is Hewlett-Packard. A company like Adaptec saves $ 10 million annually using web-based design with partners from Japan.

Approximately as much save Boeing and TRW when conducting joint research. And General Motors, working through the CommerceOne TradeXchange e-platform and selecting suppliers in fact in real time, saves about $ 400 million annually on costs.

However, in spite of the obvious advantages of Web Supply Management, there is a huge amount of uncertainty and cyber security risks. All these types of vulnerabilities and other weaknesses can leave users vulnerable to the threat being compromised or attacked. Inefficient security methods include, such as not sufficiently fast fixing of known vulnerabilities, unlimited privileged access to cloud systems, and unmanaged terminators and infrastructure.

We also consider the question: why the expansion of the Internet creates an even greater risk for organizations and their users, as well as for consumers, and what information security specialists must do now to eliminate these risks before it becomes impossible to control them.

The use of proxy servers is often an integral part of the implementation and operation of Supply Chain Management. Proxy servers have existed since the Internet inception, and their functionality has developed directly with it. Today, information security specialists use proxy servers when scanning content to identify a potential threat that are search for vulnerable Internet

infrastructures or network weaknesses that allow hackers to gain unauthorized access to Supply Chain Management, penetrate into them and conduct their campaigns.

Most of modern online advertising software in the Internet is potentially unwanted application (PUA) and is spyware. Spyware providers advertise their software as legal tools that provide useful services and adhere to end-user license agreements. Spyware disguised as PUA is software that secretly collects information about a user's computer activity. It is usually installed on a computer without the user's knowledge.

In this study, spyware is divided into three broad categories: adware, system monitors and Trojans. In a corporate environment, spyware represents a number of potential security risks. For example, it may do the following: Steal user and company information, including personal data and other proprietary or confidential information.

Reduce the effectiveness of security devices by changing their configurations and settings, installing additional software and providing access to third parties. Spyware can also potentially remotely execute arbitrary code on devices, allowing hackers to completely control the device. Increase the number of infections [34-41]. Once users are infected with PUA, such as by spyware or adware, they are vulnerable to even more malware infections

Recently, in the field of security, much attention has been paid to extortion programs. Nevertheless, another threat, by no means of such a high level, which gives its creators much more than ransomware, is the compromise of corporate e-mail. Today, this is currently the most profitable way to get a lot of money from a business. This is a deceptively light attack vector that uses social engineering to initiate theft. In the simplest version, the campaign to compromise business email includes the delivery of email to employees of

financial departments (sometimes using fake data from other employees), who can send funds via bank transfer.

Hackers usually carry out some researches in hierarchy of the companies and its employees, for example, using profiles in social networks, and build management vertical. This may be a letter from the CEO or another top manager asking him to transfer a non-cash payment to a prospective business partner or supplier. The message should motivate the recipient to send money, which as a result will usually end up in foreign or regional bank accounts owned by cybercriminals. Since messages aimed to compromise the business email do not contain malicious or suspicious links, they can usually avoid almost all the most sophisticated threat defenses.

Despite the fact that SCM in their own way are proprietary IC, they are based on free or shareware DevOps services. By this concept is meant such technologies as Docker, MySQL, MariaDB and other popular DevOps components. In January 2017, hackers began to encrypt publicly- available instances of MongoDB and demand a ransom for decryption. Later, hackers began to encrypt other types of databases, such as CouchDB and Elasticsearch. Services like DevOps services are often vulnerable because they are improperly deployed or intentionally left open to facilitate access by legitimate users. About 75% of CouchDB servers can be classified as maximally open (accessible via the Internet and do not require authentication). Only less than one quarter of them require authentication (at least entering some accounting information). As in the case of CouchDB, over 75% of Elasticsearch servers can be classified as maximally open. Unlike CouchDB, only an extremely small part of these servers may contain personal data. Docker is a software platform, whose operators from the very beginning paid great attention to security. However, despite these efforts, over 1,000 Docker instances are maximally open. Most Docker instances were found in the USA or China.

The cloud is a new area for hackers who are actively exploring it in order to gain new potential for their attacks. Hackers realize that cloud systems are vital for many Web Supply Management [42-59]. They also realize that they can break into corporate systems faster if they can break into a cloud system. Modern dynamic networks provide more opportunities for attack creating new security risks and reducing the possibility of control. The main source of such risks is the cloud. In addition, unauthorized and so -called shadow IT devices and applications create problems.

End-companies underestimate the risk (and number) of loopholes in their corporate network, cloud and end-device infrastructure. The lack of simple control leads to the fact that, on the average, from 20 to 40% of the network infrastructure and infrastructure of end-devices becomes inaccessible for analysis or management of an organization.

It is a problem that affects organizations working in the public, healthcare, and financial and technology sectors. Unmanaged network infrastructure and end devices can be easily attacked by hackers who need a base to integrate into the organization's infrastructure and compromise specific objects.

They can also be used to extract data or send unauthorized Tor traffic, or they can be part of a botnet. Even a simple router, firewall, or incorrect segmentation setting can allow a hacker to break into the infrastructure and gain access to confidential data.

The Internet of Things (Internet of Things, IoT) is the interconnection of physical devices, vehicles, buildings and other items (often called "connected devices" or "smart devices") that have built-in electronics, software, sensors, actuators and are capable to connect to the network, allowing them to collect data and share it.

IoT includes three main elements: information technology (IT), operational technology (OT) and consumer technology (CT). Industrial Internet of Things (Industrial Internet of Things, IIoT) means only connected devices within a production control network as opposed to a corporate IT network or datacenter. IoT offers great possibilities for cooperation and innovation in the business field. However, as it grows, there is the increasing of security risk of organizations and users.

One of the problems is the complexity of monitoring. Most information security specialists do not know which IoT devices are connected to their network. Security, as a rule, doesn't have top priority when creating IoT devices (and these are all devices, starting with cameras and ending with thermostats and intelligent measuring instruments).

Many of these devices are far behind in terms of security from desktop systems and have vulnerabilities fixing of which can take months or even years. In addition, they are characterized by: Vulnerability and risk reporting and updates are almost or completely missing The launch is made on a specialized architecture, The presence of non-updated or deprecated applications that have vulnerabilities, for example, Windows XP Fixing is rarely used.

The difficulty in the security issue of IoT devices is added by the fact that information security specialists may not comprehend the nature of the alarms coming from these devices. In addition, it is not always clear who among the employees in the company is responsible in case of attacks on IoT.

## 3. Conclusions

Organizations must also take the inventory devices and systems that are connected to the network. If security teams can only check with snapshots or old lists of managed devices, they can skip at least 20% of devices physically connected to the network via a wired connection. Such inventories should be

regular and automatic, as the corporate network, cloud infrastructure and end-device infrastructure are constantly changing and cannot be effectively monitored by staff manually. Today, the industry is moving to modern network connections. It is necessary to move to connected IP systems because existing systems require expensive maintenance and are complex. In addition, consumers are waiting for new secure and mobile services that the existing communication infrastructure cannot offer.

**References**

[1] Georgakopoulos, D.; Jayaraman, P.P.; Fazia, M.; Villari, M.; Ranjan, R. Internet of Things and Edge Cloud Computing Roadmap for Manufacturing. IEEE Cloud Comput. 2016, 4, 66–73.

[2] Xiao, Q.; Gibbons, T.; Lebrun, H. RFID Technology, Security Vulnerabilities, and Countermeasures. In Supply Chain the Way to Flat Organization; Intech: Vienna, Austria, 2009; pp. 357–382.

[3] Biswas, K.; Muthukkumarasamy, V.; Tan, W.L. Blockchain Based Wine Supply Chain Traceability System. In Proceedings of the Future Technologies Conference (FTC), Vancouver, Canada, 29–30 November 2017; pp. 1–7.

[4] Vinod Varma Vegesna (2021). "The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes," International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[5] Vinod Varma Vegesna (2020). "Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications," Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[6] Hamid Ali Abed Al-Asadi and et al., "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor

Network", Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[7] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[8] Hamid Ali Abed Al-Asadi, et al., "Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement", Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[9] Vinod Varma Vegesna (2019). "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[10] Pérez, L.; Dos Santos Paulino, V.; Cambra-Fierro, J. Taking advantage of disruptive innovation through changes in value networks: Insights from the space industry. Supply Chain Manag. Int. J. 2017, 22, 97–106.

[11] Keertikumar, M.; Shubham, M.; Banakar, R.M. Evolution of IoT in smart vehicles: An overview. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India, 8–10 October 2015; IEEE: Noida, India; pp. 804–809.

[12] Redondo-Gonzalez, E.; De Castro, L.N.; Moreno-Sierra, J.; Maestro De Las Casas, M.L.; Vera-Gonzalez, V.; Ferrari, D.G.; Corchado, J.M. Bladder carcinoma data with clinical risk factors and molecular markers: A cluster analysis. BioMed Res. Int. 2015, 2015, 168682.

[13] Vinod Varma Vegesna (2022). "Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues," International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[14] Vinod Varma Vegesna (2022). “Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions,” Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[15] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[16] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[17] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[18] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[19] Amador, C.; Emond, J.P.; Nunes, M.C. do N. Application of RFID technologies in the temperature mapping of the pineapple supply chain. Sens. Instrum. Food Qual. Saf. 2009, 3, 26–33.

[20] Barreto, L.; Amaral, A.; Pereira, T. Industry 4.0 implications in logistics: An overview. Procedia Manuf. 2017, 13, 1245–1252.

[21] Witkowski, K. Internet of Things, Big Data, Industry 4.0—Innovative Solutions in Logistics and Supply Chains Management. Procedia Eng. 2017, 182, 763–769.

[22] Jedermann, R.; Ruiz-Garcia, L.; Lang, W. Spatial temperature profiling by semi-passive RFID loggers for perishable food transportation. Comput. Electron. Agric. 2009, 65, 145–154.

[23] Goyal, S.; Hardgrave, B.C.; Aloysius, J.A.; DeHoratius, N. The effectiveness of RFID in backroom and sales floor inventory management. Int. J. Logist. Manag. 2016, 27, 795–815.

[24] Yang, K.; Forte, D.; Tehranipoor, M.M. Protecting endpoint devices in IoT supply chain. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, Austin, TX, USA, 2–6 November 2015; pp. 351–356.

[25] Vinod Varma Vegesna (2021). "A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments," International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[26] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[27] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[28] Vinod Varma Vegesna (2021). "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on

Cloud Computing," International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[29] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[30] Marjani, M.; Nasaruddin, F.; Gani, A.; Karim, A.; Hashem, I.A.T.; Siddiqa, A.; Yaqoob, I. Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Access 2017, 5, 5247–5261.

[31] Treiblmaier, H. The impact of the Blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Manag. Int. J. 2018, 23, 545–559.

[32] Celestine, A.; Peter, J.D. An IoT based modified graph cut segmentation with optimized adaptive connectivity and shape priors. Sustain. Comput. Inform. Syst. 2018.

[33] Lima, A.C.E.S.; De Castro, L.N.; Corchado, J.M. A polarity analysis framework for Twitter messages. Appl. Math. Comput. 2015, 270, 756–767.

[34] Griffiths, F.; Ooi, M. The fourth industrial revolution-Industry 4.0 and IoT [Trends in Future I&M]. IEEE Instrum. Meas. Mag. 2018, 21, 29–43.

[35] Suresh, P.; Daniel, J.V.; Parthasarathy, V.; Aswathy, R.H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Proceedings of the International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India, 27–29 November 2014; pp. 1–8.

[36] Li, X.; Wang, Y.; Chen, X. Cold chain logistics system based on cloud computing. Concurr. Comput. Pract. Exp. 2012, 24, 2138–2150.

[37] Saragih, L.R.; Dachyar, M.; Zagloel, T.Y.M.; Satar, M. The Industrial IoT for Nusantara. In Proceedings of the 2018 IEEE International Conference on

Internet of Things and Intelligence System (IOTAIS), Bali, Indonesia, 1–3 November 2018; pp. 73–79.

[38] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106.

[39] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[40] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[41] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[42] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[43] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[44] Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horiz. 2015, 58, 431–440.

[45] Obitko, M.; Jirkovský, V.; Bezdíček, J. Big data challenges in industrial automation. In Proceedings of the International Conference on Industrial Applications of Holonic and Multi-Agent Systems, Prague, Czech Republic, 26–28 August 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 305–316.

[46] Chaudhuri, A.; Dukovska-Popovska, I.; Chan, H.K.; Subramanian, N.; Bai, R.; Pawar, K.S. Development of a framework for big data analytics in cold chain logistics. In Proceedings of the International Symposium on Logistics, Kaohsiung, Taiwan, 3–6 July 2016; Centre for Concurrent Enterprise, Nottingham University Business School: Nottingham, UK, 2016; pp. 498–506.

[47] Waller, M.A.; Fawcett, S.E. Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management. J. Bus. Logist. 2013, 34, 77–84.

[48] Rejeb, A. Blockchain Potential in Tilapia Supply Chain in Ghana. Acta Tech. Jaurinensis 2018, 11, 104–118.

[49] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[50] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, "Fuzzy Logic approach to Recognition of Isolated Arabic Characters", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[51] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[52] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[53] Cam-Winget, N.; Sadeghi, A.-R.; Jin, Y. INVITED: Can IoT be Secured: Emerging Challenges in Connecting the Unconnected. In Proceedings of the 53rd Annual Design Automation Conference (DAC ’16), Austin, TX, USA, 5–9 June 2016.

[54] Lu, W.; Huang, G.Q.; Li, H. Scenarios for applying RFID technology in construction project management. Autom. Constr. 2011, 20, 101–106.

[55] Rejeb, A. The Potentialities of RFID-Based Traceability System in the Olives Post-Harvest Stage. J. Bus. Manag. Econ. Res. 2018, 2, 13–25.

[56] Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. Wireless Sensor and Actuator Networks: Technologies, Analysis and Design; Elsevier: Amsterdam, The Netherlands, 2008.

[57] Wang, S.J.; Liu, S.F.; Wang, W.L. The simulated impact of RFID-enabled supply chain on pull-based inventory replenishment in TFT-LCD industry. Int. J. Prod. Econ. 2008, 112, 570–586.

[58] Zhou, Z. Applying RFID to reduce bullwhip effect in a FMCG supply chain. In Proceedings of the Advances in Computational Environment Science, Australia, Melbourne, 15–16 January 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 193–199.

[59] Newman, D. How IoT Will Impact The Supply Chain. Available online: https://www.forbes.com/sites/.